On July 31, 2018, the City Council, in accordance with the Surveillance Technology Ordinance adopted, the following Crisis Negotiations Equipment Use Policy (26.07.030 Davis Municipal Code)

**Surveillance Use Policy**

Crisis Negotiations Equipment – The equipment consists of a command module, two laptop computers that are used to run the software programs and record audio/video of the incident, and a “throw phone.” The equipment is manufactured by 836 Technologies and is widely used throughout the region and country for use in crisis negotiation communications. For evidentiary purposes, negotiations must be audio recorded. The majority of negotiations are accomplished by calling the person on the phone. In some cases it is necessary to provide the person with the “throw phone”. The throw phone is essentially a phone in a protective case with a very long phone cord attached to it.

(a) **Purpose:** The specific purpose(s) that the surveillance technology item is intended to advance.

The safe negotiation and eventual surrender of a person in crisis without injury to them, hostages, officers or members of the public.

(b) **Authorized Use:** The uses that are authorized, and the rules and processes required prior to such use.

Those authorized to use the equipment must be members of the Yolo County Crisis Negotiations Team (CNT). Those team members are trained how to use the equipment.

(c) **Data Collection:** The information that can be collected by the surveillance technology, including “open source” data.

The technology records audio and potentially video of the incident. The technology does not use “open source” data.

(d) **Data Access:** The category of individual who can access or use the collected information, and the rules and processes required prior to access or use of the information.

Any member of the Yolo County CNT can access the data during the incident. At the conclusion of the event, the data is stored on a CD and that CD is then booked into evidence at the Davis Police Department.
(e) Data Protection: The general safeguards that protect information from unauthorized access, including encryption and access control mechanisms. Nothing in this subsection shall be construed to require the disclosure of information that could reveal vulnerabilities to, or otherwise increase the potential for an attack on, an information technology system of the City.

Only those CNT members who are trained to use the equipment can access the data. Once the data is put on a CD, only those members who would normally have access to evidence would be able to access the data.

(f) Data Retention: The time period, if any, for which information collected by the surveillance technology will be routinely retained, the reason such retention period is appropriate to further the purpose(s), the process by which the information is regularly deleted after that period lapses, and the specific conditions that must be met to retain information beyond that period.

The data is considered evidence. The time period the data would be retained would be dictated by the court process.

(g) Public Access: How collected information can be accessed or used by members of the public, including criminal defendants.

The general public would not have access to the data. If criminal charges are filed against the person, they would have access to a copy of the data booked into evidence. The copy of the data is provided to the defendant through their attorney.

(h) Third Party Data Sharing: If and how other City or non-City entities can access or use the information, including any required justification or legal standard necessary to do so and any obligations imposed on the recipient of the information.

The technology does not use Third Party Data Sharing.

(i) Training: The training required for any individual authorized to use the surveillance technology or to access information collected by the surveillance technology.

Several members of the CNT were initially trained by the manufacturers of the technology. The technology is used on an on-going basis.

(j) Auditing and Oversight: The mechanisms to ensure that the Surveillance Use Policy is followed, including internal personnel assigned to ensure compliance with the policy, internal record keeping of the use of the technology or access to information collected by the technology, technical measures to monitor for misuse, any independent person or entity with oversight authority, and the legally enforceable sanctions for violations of the policy.

The technology and the storage of the data is supervised and managed by the Davis Police Department Sergeant and Lieutenant assigned to the CNT.

Darren Pytel
Police Chief
July 31, 2018